

ЗАЩИТА, СОХРАНЕНИЕ И ВОССТАНОВЛЕНИЕ ИНФОРМАЦИИ

Ни шанса для воров




Здесь представлено продолжение материала статьи «Ни единого шанса для вора» (см. ЧИП 8/99, с. 94). В этой части статьи вы узнаете о применении программы PGP, безопасности данных, работе с паролями и восстановлении информации

Для обеспечения секретности и безопасности передаваемой информации необходимо использовать программы шифрации/дешифрации данных. Среди этих программ наибольшей популярностью пользуется программа PGP. Защита данных на компьютере невозможна без приме-

нения различных паролей, а для восстановления случайно или ошибочно удаленных данных требуется соответствующее программное обеспечение.

Здесь вы узнаете, как правильно применять встроенные возможности Windows и специальных программ для защиты своих данных.

СОДЕРЖАНИЕ

Защита данных	94
Pretty Good Privacy	8/99 
Проблемы с паролем	8/99 
Восстановление данных ...	8/99 

Pretty Good Privacy

Программа PGP — это очень надежный способ кодирования, основанный на системе так называемых личных (частных) и публичных (общедоступных) ключей. Вы зашифровываете почтовое сообщение с помощью публичного ключа получателя, который для

этого также должен пользоваться PGP. Получатель может расшифровать сообщение только с помощью своего личного, известного лишь ему ключа. С помощью опции *Sign* вы добавляете в личный ключ свою подпись. Благодаря этому получатель может проверить, дей-

ствительно ли вы являетесь отправителем почтового сообщения. Для этого он должен получить публичный ключ.

Программа кодирования из Internet

Для частного пользования PGP существует в виде Freeware-программы

только на английском языке. Текущую версию можно получить по адресу www.pgpi.com/download. Версия для Windows 95/98/NT содержит подключаемый элемент для Eudora Light 3.0, Eudora Pro 4.0, Microsoft Exchange и Outlook 97. Для пользователей Outlook Express также существует подключаемый элемент, который нужно загружать извне.

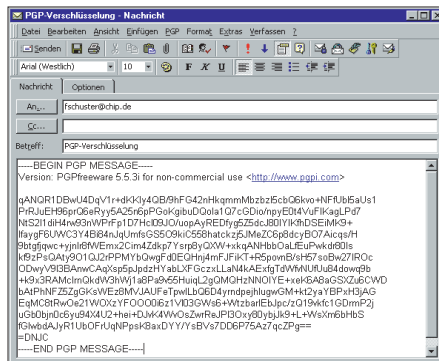
В Internet можно найти и американскую версию PGP 6.0.2, которую нельзя загрузить вне США из-за закона, связанного с экспортом криптографических программ из этой страны. Более подробно об этом во вставке внизу.

Применение PGP

После успешной инсталляции первым делом следует создать Public Key (публичный ключ) и Private Key (закрытый ключ). При этом пользователь имеет поддержку так называемого мастера генерирования ключей (Key Generation Wizard).

Длина кода выбирается произвольно и максимально может быть 4096 бит. Впоследствии безопасность данных тем выше, чем длиннее и сложнее произвольно выбранная фраза-пароль, о которой вас спрашивают в следующем диалоговом поле. На следующем этапе вы отказываетесь от возможности передать код на Key-сервер, поскольку обычно он не работает.

Теперь можно начинать работу. В зависимости от типа используемого поч-



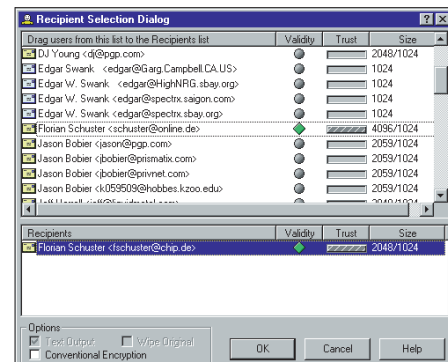
PGP-криптография бесплатно: только правильный пароль делает видимым первоначальный текст

того клиента необходимо еще инсталлировать соответствующий подключаемый элемент. Щелкните в программе электронной почты на кнопке *Encrypt message before sending*. Теперь, если начать процесс передачи почты, сообщение и вложенные в него файлы будут закодированы.

Наиболее надежный способ — это асимметричное кодирование сообщений электронной почты. При этом PGP запрашивает вас о получателе сообщения (*Recipient*). Если же вы еще не получили от адресата публичный ключ, то остается только симметрично защитить почту произвольно выбранным паролем. Для этого нужно выбрать строку *Conventional Encryption*.

Безопасность данных

Недостатком симметричного способа кодирования является то, что получателю нужно специально сообщить пароль



Максимальная надежность: перед кодированием электронной почты нужно выбрать получателя

по телефону или по электронной почте. Однако это вносит в очень надежный способ кодирования не просчитываемый коэффициент риска. Поэтому везде, где это возможно, следует пользоваться асимметричным способом.

Совет ЧИПа: Щелчок правой кнопки мыши на имени получателя в модуле PGPkeys откроет контекстное меню, команда *Export...* которого позволит сохранить код в текстовом файле, который затем можно передать по электронной почте.

На практике это выглядит следующим образом: вы экспортируете публичный ключ и передаете его дальше, ваш партнер по электронной почте делает то же самое и посылает вам свой публичный ключ. Таким образом, больше ничего не препятствует безопасному обмену данными между вами.

Кодирование данных в буфере обмена

С помощью программы PGP можно не только кодировать сообщение электронной почты, но обеспечить безопасность своих файлов. Если вы не «опубликовали» свой публичный ключ, то декодировать данные можете только вы сами. Благодаря этому PGP обеспечивает очень высокий уровень безопасности (по нашей классификации соответствует третьему уровню защиты). Если вы хотите использовать PGP как для кодирования электронной почты, так и для решения местных задач, то лучше всего создать вторую пару кодов для шифровки файлов.

Например, для зашифровки текстового фрагмента документа нужно поступить следующим образом: с помощью комбинации клавиш [Ctrl]+[C] скопируйте текст в буфер обмена. Щелкните кноп-

Как был обойден запрет США на экспорт технологии кодирования



Со времен второй мировой войны из США без разрешения нельзя экспортировать технологии кодирования, длина кода которых превышает 56 бит. Поскольку программа Pretty Good Privacy основана на коде длиной 128 бит, то она также подлежит этому строгому запрету. Разработчику PGP, компании Network Associates, удалось распространить свой продукт по всему миру только благодаря небольшой уловке. В Конституции США с 1791 г. жестко закреплено право на свободу выражения мнения («freedom of speech»). В соответствии со статьей 1 билля о правах это право не может быть ограничено никаким законом. Согласно

действующей юрисдикции утверждает, что под это право попадают также все печатные произведения. Таким образом, компания Network Associates напечатала и издала все исходные коды PGP. Через подставное лицо книги были закуплены в книжных магазинах Сан-Франциско и легально экспортированы в Швейцарию, где коды были заново зарегистрированы и компилированы.

Эта, теперь уже европейская программа, может быть продана Network Associates. Так как сбыт криптографической программы из Голландии, основного места местонахождения этой компании в Европе, не может быть неограниченным, то частично ее выпускают в Ирландии.

кой мыши на небольшой пиктограмме *PGPTray* в системной строке линейки задач (рядом с указателем времени).

После этого выберите функцию *Encrypt Clipboard*. В раскрывшемся диалоговом поле выберите в качестве получателя самого себя или же активируйте опцию *Conventional Encryption* и щелкните на кнопке *OK*. В последнем случае можно ввести собственный пароль специально для этого текста. После этого в буфере появится зашифро-

ванная версия вашего текста, которую снова можно ввести в общий текст с помощью комбинации клавиш [Ctrl]+[V].

Надежное кодирование файлов на собственном ПК

Через контекстное меню любого файла или в любом каталоге (правая кнопка мыши) в окне Проводник существует возможность закодировать файлы (*PGP/Encrypt*). При этом имена файлов остаются без изменений. Это дает

возможность найти нужный файл, но, в то же время, и облегчает работу вора.

Также не следует забывать об удалении «старых» незакодированных файлов. Для этого следует либо активировать в первом диалоговом окне опцию *Wipe Original*, либо удалить файлы вручную. Однако не всегда удаленные файлы действительно исчезли. В PGP также есть для этого соответствующая функция *PGP/Wipe* в контекстном меню.

Проблемы с паролем

Если вы работаете с паролями, то по сути имеете дело с паролями трех типов: пароли для сообщений в операционной системе (например, Windows for Workgroups, Windows 95/98/NT), для локальной сети (домен Windows) или для провайдера Internet.

Совет 7: Пароли Windows 95/98 — неэффективная защита*

Сначала наиболее часто встречающийся случай: пароли для Windows for Workgroups и Windows 95/98. В случае этих паролей речь не идет о собственном пароле — вместе с именем пользователя они служат лишь для идентификации пользователя. По классификационной шкале от 1 до 3 баллов эти пароли соответствуют только первому уровню защиты.

Это можно легко проверить. Сначала перезагрузите ПК. В диалоговом окне запроса введите в качестве имени пользователя любое слово. Windows не знает пользователя с таким именем, и поэтому создаст новую пользовательскую учетную запись. Далее последует запрос выбора пароля. После ввода пароля вы будете

иметь полный доступ к локальному ПК.

Правда, новый пароль пригоден только для обращения к данному ПК. Для доступа к сетевым ресурсам требуется еще и сетевой пароль (в зависимости от конфигурации сети).

Windows сохраняет такие пароли в PWL-файлах, которые существуют в закодированном формате. Правда, при этом тоже речь идет только о первом уровне защиты, поскольку в Internet существуют программы для взлома PWL-файлов. Одна из таких программ находится по адресу www.ntsecurity.net/security/pwl.htm. В Windows NT дела не лучше. Хотя расшифровка паролей и представляет некоторые трудности, но она вполне возможна.

По адресу www.L0pht.com находится программа *L0phtcrack*, которую можно использовать для взлома NT-паролей. На практике, если вы полностью положились на защиту паролем и при этом забыли его, то возникает довольно сложная ситуация. *L0phtcrack* работает со списком слов, которые программа варьирует в произвольном порядке.

Кроме того, для NT-сетей (и других локальных сетей) существуют так называемые анализаторы паролей, которые «прослушивают» работу сети и вылавливают оттуда учетные записи и пароли.

Пользователям нужно помнить о том, что пароли в Windows

Как выглядят надежные пароли

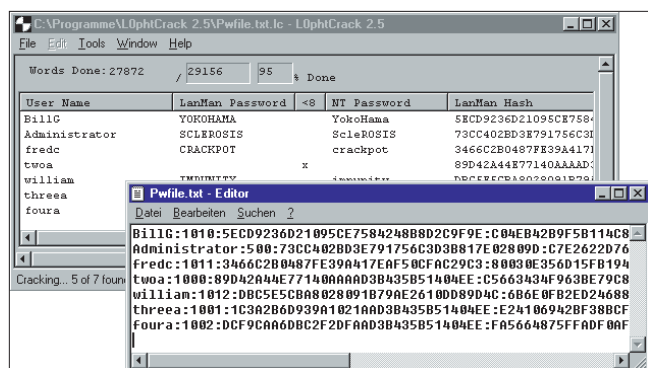
Для того чтобы воспользоваться расширенными технологиями защиты паролем, необходимо лишь следовать нескольким простым правилам. Надежный пароль состоит по крайней мере из 8 символов. Не используйте при этом слова, которые можно найти в словаре. Неприспособно и только число, например, дата дня рождения. Наибольшей безопасности можно добиться при использовании длинного пароля, который состоит из произвольной последовательности букв, цифр и, еще лучше, специальных символов. Кроме того, обычно при запросе пароля различаются заглавные и строчные буквы. Таким образом, если дополнительно использовать заглавные и строчные буквы, то отгадать пароль будет практически невозможно. Таким образом можно усложнить жизнь большинству хакерских программ. Например, при использовании *L0phtcrack* для взлома восьмизначного пароля, содержащего два специальных символа, требуется примерно 600 часов работы ПК с процессором Pentium-II/350, а так долго программа вряд ли может работать на чужом компьютере незаметно для его владельца.

NT обеспечивают лишь второй уровень защиты.

Совет 8: BIOS-пароль защищает ПК

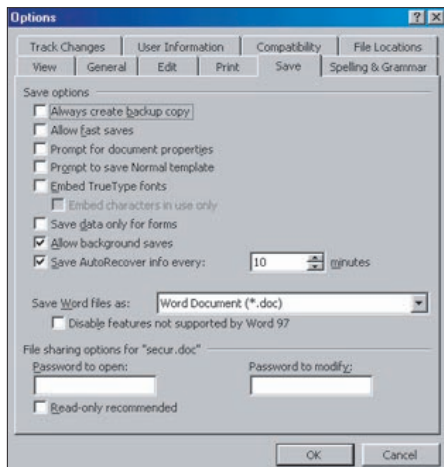
Каждый ПК имеет встроенную защиту паролем, которая является относительно надежной. В BIOS-Setup ПК можно указать, чтобы при каждой загрузке эта система запрашивала пароль.

Поскольку этот запрос происходит до загрузки операционной системы, то без знания правильного слова шансы получить доступ к ПК в какой-либо форме относительно невелики. Если же вы забыли свой пароль, то остается



NT-пароль легко взломать: любой пользователь может загрузить из Internet программу L0phtcrack

*Советы 1—6 находятся в ЧИП 8/99 на стр. 94



Обманчивая безопасность: в Word документы можно защитить паролем — правда, этот пароль ненадежен

ся только один путь: на материнской плате компьютера находится небольшая батарея. Если отключить ее, то BIOS «забудет» все установки, в том числе и пароль.

Совет 9: Online-пароли

Параметры обращения к провайдерам Internet, так же как и учетные записи операционной системы и сети, состоят из имени пользователя (для идентификации доступа) и соответствующего пароля.

В настоящее время провайдеры Internet чаще всего используют протокол PPP (Point-to-Point Protocol), который в свою очередь имеет несколько альтернативных механизмов для идентификации доступа.

По возможности не пользуйтесь СНАТ-механизмом (в сетях передачи данных под управлением Windows 95/98 вкладка *Script*), поскольку при этом пароль передается по телефонной

сети незашифрованным. В отличие от этого альтернативные механизмы PAP (Password Authentication Protocol) и CHAP (Challenge Handshake Authentication Protocol) предварительно зашифровывают особо важные элементы онлайн-передачи. Критично обстоят дела в таких онлайн-офисных службах, которые используют собственный механизм доступа со специальным программным обеспечением, которое сохраняет параметры доступа на жестком диске.

Например, существует Freeware-программа (Password Detective for AOL от Tricos Software), которая вывела AOL-пароли у большинства клиентов AOL.

Вы можете воспользоваться такой программой-взломщиком, если забыли свой собственный Online-пароль.

Совет 10: Психология вместо программы взлома

Пытаясь сохранить данные в тайне, кое-что все равно нужно постоянно держать перед глазами. Большинство взломов файлов происходит с использованием элементов психологии. Зачем использовать дорогие программы для «взлома» пароля, если все делается гораздо проще? Например, в качестве пароля для защиты данных часто используется имя друга или даже кличка любимого кота. Поэтому в первую очередь выполните следующее правило: придумайте свой собственный пароль в самом настоящем смысле этого слова.

Поскольку пароли трудно запомнить, то многие пользователи их записывают. Очень часто секретная записка с паролем лежит под клавиатурой или приклеена на обратной стороне монитора. В таких условиях ее проще показать коллегам.

Довольно просто добраться до пароля извне: сотрудник внешне вызывается в отдел электронной обработки данных и оттуда сообщает, что установлены новые серверы. Необходимо передать паро-

ли, в противном случае, начиная со следующего дня, сообщения перестанут поступать. Очень жаль, но старые серверы уже не работают. Поэтому нужно как можно быстрее узнать старые имена пользователей и пароль, чтобы сконфигурировать новый компьютер.

Таким образом, если запрашивают ваш пароль, нужно быть предельно осторожным! Ни один серьезный системный администратор не будет спрашивать пользователя о его пароле по телефону или через электронную почту.

Совет 11: Простое решение для знающих

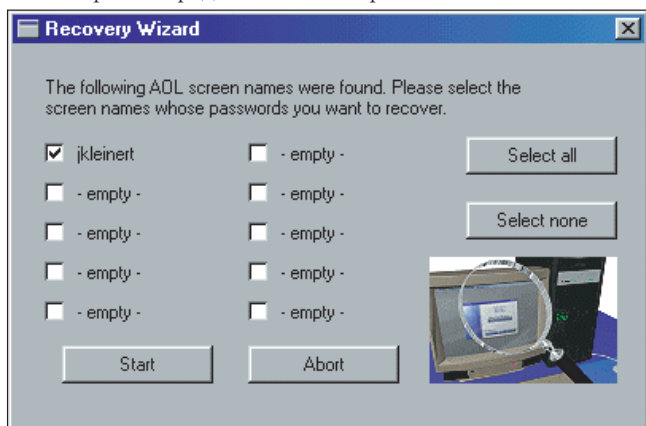
В связи с тем, что пароли операционной системы не представляют никакого серьезного препятствия для хакера, неудивительно, что и пароли таких программ, как Excel, Word Perfect или Quicken, не годятся в качестве средства защиты.

Такие пароли защищают исключительно от неопытных пользователей. Технически грамотный пользователь просто обратится, например, по адресу www.accessdata.com, заказав дешифраторы для наиболее популярных программ. В Internet также нет недостатка во Freeware-программах.

Как правило, существует средство и против данных, защищенных паролем, чей алгоритм не так-то просто просчитать: благодаря длинному списку слов и взламывающим программам особо терпеливые шпионы вполне могут подобраться к вашим данным. Еще проще это сделать, если частично известно содержимое искомым файлам.

Точно такие же механизмы вы, уже как не-хакер, можете использовать для своих собственных данных, если забыли пароль. К программам этой группы относятся, например, Zip- и ARJ-архивы.

Соответствующие программы можно найти в Internet по адресу www.sud-denddeath.fsn.net. Здесь же можно прочитать и о санкциях в случае злоупотребления этими программами. Обширная библиотека по утилитам для хакеров находится по адресу <ftp://ftp.ox.ac.uk/pub/crypto/cryptanalysis>. Тем не менее, «взламывайте» только свои собственные файлы.



AOL-пароль взломан: если вы хоть раз сохранили AOL-пароль в AOL-Client, то он стал легкой добычей для такой программы взлома, как Password Detective

Восстановление данных

Будет очень неприятно, если вы случайно удалите еще нужные вам данные. В зависимости от важности утерянных данных иногда имеет смысл затратить некоторые усилия на восстановление всего файла или его части.

Иногда это делается легче, чем вы думаете: многие данные, которые вы как будто удалили, на самом деле не уничтожены, а еще находятся на жестком диске. Кроме того, пользовательские программы некоторое время сохраняют в документе удаленные данные.

Совет 12: Спасение данных

Если вы работаете в редакторе Word с конфиденциальным текстом и ненадолго покидаете рабочее место, то недостаточно временно удалить из текста «щекотливые места»: пока Word еще работает, любой может вызвать на экран удаленные фрагменты с помощью команды *Edit/Undo*.

Это всего лишь простой пример, но он характерен для категории «на самом деле неудаленных данных». Результат очевиден: вы точно так же легко можете восстановить свои удаленные данные, как и любопытный шпион.

Другой пример: Outlook Express по умолчанию заносит удаленные письма в каталог *Deleted Items*. После того, как вы прочитали почту и удалили ее, она все еще абсолютно доступна из почтовой программы. Даже если закрыть Outlook, все равно почта на самом деле не удаляется. Впоследствии любой может запустить Outlook и просмотреть каталог *Deleted Items*.

Однако существует простой способ, позволяющий избежать этой ловушки. Во вкладке *Tools/Options/Mainte-*

nance установите опцию, чтобы каталог *Deleted Items* автоматически очищался по окончании работы Outlook, в противном случае все нужно тщательно удалить вручную.

Совет 13: Корзина Windows так же надежна, как и мусорное ведро

Все вышесказанное справедливо и для Windows: если вы удалили файл с помощью окна Проводник, то на самом деле он не удален с жесткого диска, а просто перенесен в *Корзину*. Оттуда файл можно восстановить в любое время. Это очень удобно, если файл удален по ошибке. Правда, любой другой пользователь также может выудить из корзины соответствующий файл.

Естественно, наиболее простое решение — это просто всегда очищать корзину с помощью правой кнопки мыши. Очистка корзины означает лишь логическое удаление файла из файловой системы, но не его физическое уничтожение.

Профессионалу не составит большого труда заново составить эти данные и восстановить первоначальный файл.

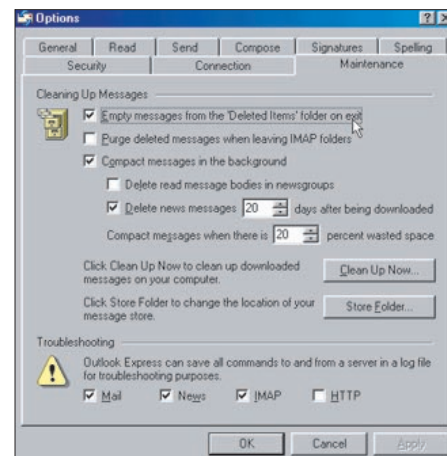
Все вышесказанное относится и к файлам, удаленным в DOS-окне с помощью команды *del*. В MS-DOS имеется программа Undelete, выполняющая эту задачу для своих владельцев. Правда, в Windows 98 такого рода программ больше нет, однако в этом случае поможет такая Shareware-программа, как Revival (<http://user.chollian.net/~ship3>). Эта утилита может восстановить файлы даже в том случае, если удален их каталог или же в FAT «поработал» вирус.

Удаленные файлы легко узнать в Revival-окне: они зачеркнуты красной линией. Для их восстановления щелкните правой кнопкой мыши на выбранном файле и в контекстном меню выберите команду *Save*.

Совет 14: Просмотр уничтоженных данных

С помощью обычного редактора диска, например Diskedit от PTS или Norton Diskedit, можно заглянуть в глубины вашего жесткого диска.

► Создайте простой текстовый файл, в котором содержится текст, о котором



Безопасный случай: Outlook Express автоматически уничтожает удаленную почту только в том случае, если вы поставите эту галочку. Эта установка проводится вручную даже в Outlook 97/98

вы точно знаете, что его нет на жестком диске.

► Удалите файл вручную в окне Проводник и с помощью редактора диска выполните поиск текста (собственно говоря, удаленного) файла. Достаточно даже одного ключевого слова, чтобы фрагменты содержимого удаленного файла снова появились на экране. Однако будьте осторожны: работая с таким редактором на жестком диске, можно его случайно удалить. Осуществляйте только такие действия, в последствиях которых вы совершенно уверены.

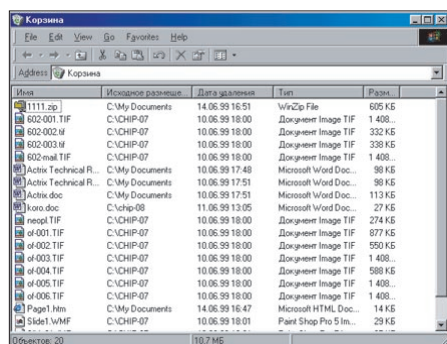
Совет 15: Восстановление данных в Linux

Как правило, Linux-системы работают с файловой системой Ext2. Существует программа для интерактивного просмотра и работы с этой файловой системой: *debugfs*. Будьте осторожны, в этом случае, так же как с Diskedit в DOS или Windows, можно уничтожить данные любых размеров. На такое вмешательство может решиться только тот, кто умеет обращаться с этой программой.

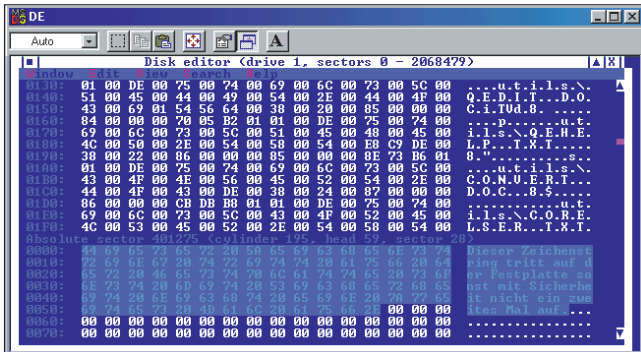
Совет 16: Воссоздание утерянных данных из swap-файла

Если важный документ удален безвозвратно, то существует несколько возможностей спасти небольшие его фрагменты.

► Если «несчастье» произошло только что, создайте копию swap-файла Windows, обычно *c:\win386.swap*.



Корзина — это обычный каталог: все удаленные файлы просто перемещаются в корзину



Жесткий диск под лупой: редактор диска снова находит на диске удаленные файлы

Этот метод срабатывает только в MS-DOS-режиме. Обратите внимание на то, чтобы на жестком диске было достаточно места. Кроме того, swar-файл является скрытым.

Windows сохраняет в swar-файле содержимое основной памяти блоками по 4 КБ. Вы найдете здесь фрагменты информации в зависимости от заполнения оперативной памяти и использования ресурсов.

- Используйте Нех-редактор, например Нех-Wizard, и откройте копию swar-файла. Найдите известные строки символов и скопируйте найденные фрагменты через буфер обмена в текстовый файл. Позже их можно будет отредактировать вручную.

Этим способом охотно пользуются хакеры, например для поиска паролей на жестком диске. Естественно, чем дольше работают на ПК с момента утери данных, тем меньше вероятность успешного поиска.

Совет 17: Восстановление данных с помощью Windows

Щелкните правой кнопкой мыши на пиктограмме жесткого диска и из контекстного меню выберите команду *Свойства/Сервис/Выполнить проверку*.

Если появилось сообщение об утерянных элементах, то их нужно обязательно преобразовать в файлы в корневом каталоге. Позже их можно открыть с помощью редактора и попытаться составить искомую информацию.

Совет 18: Компоновка разрушенных элементов с помощью Diskedit

С помощью редактора Diskedit можно собрать файл поэлементно (точнее, покластерно). Например, с помощью

PTS-Diskedit это делается следующим образом:

- Создайте текстовый файл, по объему больший, чем файл, который хотите восстановить. Создайте текстовый файл с единственным предложением, например, «Кошка поднимается по винтовой лестнице».

- Вызовите PTS-Diskedit и в шестнадцатеричной записи попытайтесь найти те строки символов, которые нужно найти в утерянном файле. Выделите весь кластер и скопируйте его в буфер обмена (команда *Edit/Copy*).
- Теперь создайте новый файл, введите содержимое буфера в этот файл и сохраните его. Повторите игру: утерянный кластер 1, утерянный кластер 2 и так для всех кластеров.

Совет 19: Склеивание в Norton Diskedit разрушенных кластеров

Редактор дисков Norton Utilities, работающий только под управлением DOS или в DOS-режиме Windows, несколько удобнее.

- Выполните поиск строки символов утерянного файла в текстовой форме, пометьте содержание кластера и вызовите *Tools/Write Object To/to a File*.
- Теперь выделенную часть можно просто сохранить в новом файле. Повторите процесс, как и при работе с PTS, до тех пор, пока не составите вместе наибольшее число кластеров или все кластеры.

С помощью Norton Diskedit можно определить даже каталоги и файлы, а затем с помощью клавиши [Enter] перейти к неразрушенным кластерам. При знании структуры FAT пользователям Norton работать еще легче, так как эта программа показывает даже связи в FAT, хотя

они еще не были переписаны в новых записях.

Правда, описанный способ несколько сложен, поэтому рекомендуется только для опытных пользователей.

Совет 20: Восстановление отформатированной файловой системы

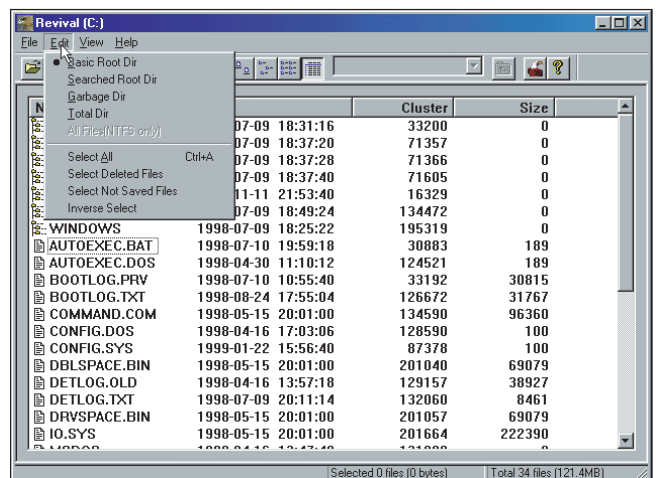
Если вы работаете невнимательно, то может так случиться, что вместо дискеты вы отформатируете жесткий диск. Не волнуйтесь: с помощью программы *Unformat* из пакета Norton Utilities или уже описанной программы *Revival* можно все восстановить.

По этому же принципу действуют и хакеры: если им в руки попадает Quick-форматированная, т. е. кажущаяся пустой, дискета, то с помощью программы *Unformat* они могут снова увидеть записанные на ней ранее файлы. Точно так же могут поступить и в том случае, если вы продали кому-то постороннему свой жесткий диск. Поэтому не передавайте чужим свои Quick-форматированные носители данных.

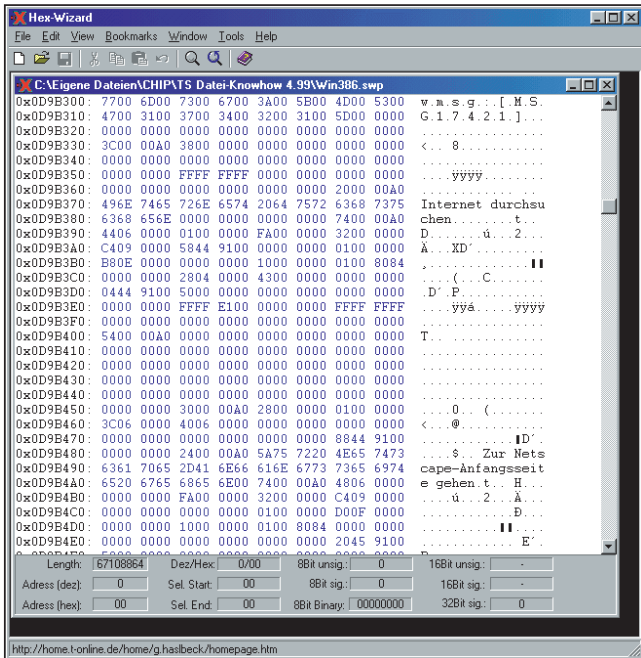
Совет 21: Восстановление поврежденной таблицы сегментов

Гораздо сложнее обстоят дела, если повреждена таблица сегментов. Причиной этого могут быть вирусы или проблемы с устройствами ПК. Если, например, в BIOS-Setup записаны неправильные геометрические параметры жесткого диска или установлен другой режим для подсчета секторов, то наступает настоящий хаос.

Единственный надежный выход соз-



Удаленные файлы «вытащены из шляпы»: shareware-программа Revival может сделать это даже в том случае, если удалена соответствующая директория



Взгляд в swp-файл Windows: здесь можно найти некоторую информацию, например, даже после сбоя системы

дает профилактическая мера: сохранение Master Boot Records (MBR), включая таблицу сегментов, на дискете. Владельцы Norton Utilities создают для этого Rescue-дискету, при этом нужно воспользоваться программой инсталляции. Если случилась такая напасть, загрузите компьютер с дискеты и выполните программу *Rescue*, которая прохо-

дит в диалоговом режиме. Лучше всего пользоваться загрузочной дискетой DOS или Windows, на которой записан файл STP.EXE.

Совет 22: Восстановление таблицы сегментов в Linux

Для пользователей Linux также существует помощь на крайний случай.

Фанаты Shareware используют *Save The Partition!* — программу, которая относится к инструментальным программам сохранения данных (STBFP версия 2.0 находится по адресу www.easy-net.on.ca/blue-fox/stbfp.html).

Команда STP 1 A:\MBR.STR /S/O записывает MBR первого диска на дискету в файл MBR.STR. В случае повреждения с помощью команды STP 1 A:\MBR.STR /R можно переписать содержание файла

назад на сектор диска. Команда STP 1 A:\MBR.STR /S/O записывает MBR первого диска на дискету в файл MBR.STR. В случае повреждения с помощью команды STP 1 A:\MBR.STR /R можно переписать содержание файла

Используйте в своей системе отформатированную дискету, например, в качестве каталога /floppy.

С помощью команды

```
dd if=/dev/hda of=/floppy/mbr size=512 count=1
```

можно сохранить на дискете MBR и таблицу сегментов. Если кто-то называет SCSI-диск по-своему, то нужно заменить *hda* на *sda*. Если MBR имеет дефекты, то нужно загрузить компьютер с дискеты Linux, вытащить ее, вставить дискету с файлом *mbr*, отработать ее и ввести команду

```
dd if=/floppy/mbr of=/deb/hda size=512 count=1.
```

Совет 23: Без резервной копии данных

Возможно, до настоящего времени вы упустили из виду создание резервной копии MBR. Если в таком случае произошло разрушение таблицы сегментов, то спасти данные труднее, но все-таки можно.

Сначала нужно выяснить, умеете ли вы работать с такими программами, как Norton Diskdoctor или Scandisk для Windows. Будьте осторожны: если эти программы неправильно интерпретируют существующие ошибки, то они нанесут больше вреда, чем пользы.

Таким образом, если доступа к жесткому диску нет из-за предполагаемых дефектов сегментов, то упомянутые программы ни в коем случае не должны восстанавливать утерянные сегменты. Попробуйте просто восстановить MBR и таблицу сегментов. Лучше всего предварительно создать копию этого начального сектора жесткого диска.

► Если восстановление с помощью программного обеспечения не удалось, то остается только еще раз попытаться своего счастья. При этом, если у вас мало опыта работы с ПК, то лучше всего заручиться поддержкой опытного пользователя.

► Просмотрите в BIOS-Setup геометрические параметры жесткого диска (цилиндр, головки, количество секторов на дорожку) и запишите эти данные.

► Загрузите компьютер с загрузочной DOS-дискеты, на которой также находится Diskedit от PTS или Norton Utilities.

► Выберите физически существующий диск (вероятно, это будет первый

Переписанные данные защищены от хакеров

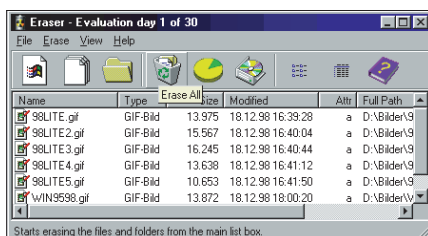
Воспрепятствовать хакерам повторно воспользоваться информацией после ее удаления может только перезапись удаленных данных на жесткий диск с другим обозначением.

Некоторые разработчики предлагают специальные коммерческие инструментальные программы по уничтожению данных. Одной из наиболее популярных программ является, например, Eraser от East-Tec (www.east-tec.com) по цене \$30. Если речь идет только об удалении дан-

ных, то можно воспользоваться Pretty Good Privacy (PGP). Программа распространяется бесплатно и может, совершенно между делом, закодировать файлы и электронную почту. Поскольку Freeware существует только в англоязычной версии, то многие пользователи боятся ее применять. Однако для удаления файлов пользоваться ею достаточно просто: PGP полностью встраивается в Проводник Windows, так что нужно только вызвать PGP/Wipe через контекстное меню.

Большинство коммерческих программ кодирования содержат модуль, надежно удаляющий файлы. Таким образом, даже амбициозные хакеры не смогут восстановить ваши конфиденциальные данные.

Если вы пользуетесь NTFS (NT File System), то не нужно никакой специальной программы: при удалении файлов из корзины NT самостоятельно переписывает информацию с жесткого диска.



Высший уровень защиты: Eraser от East-Tec безвозвратно удаляет файлы с жесткого диска

Disk editor (drive 1, sectors 0 - 8916874)

Window Edit View Search Help

Absolute sector 0 (cylinder 0, head 0, sector 1)

BootWizard hidden partitions: Unused
Unused
Unused
Unused

BootWizard boot disk: 000h
BootWizard boot sector: 0
BootWizard boot partition: 0
BootWizard checksum: 000h
BootWizard structure size: 0
Windows NT serial number: 000000000h
BootWizard serial number: 00000h

Type	Boot	Starting loc	Ending loc	Relative sectors	Number of sectors
		Cyl Head Sec	Cyl Head Sec		
Win95 FAT-32	No	0 1 1	254 254 63	63	4096512
LINUX Swap, Solari	No	255 0 1	262 254 63	4096575	128520
Extended	Yes	263 0 1	838 254 63	4225095	1220940
Unused	No	0 0 0	0 0 0	0	0

Partition table signature (00A55h): 00A55h

Если ничего не получается: ручная работа над таблицей сегментов с помощью Diskedit только для профессионалов

диск), с которым возникли проблемы. Перейдите в первоначальный сектор жесткого диска (для PTS — команда *Search/Goto begin*) и переключитесь, если это необходимо, на режим отображения таблицы сегментов.

- Сравните данные таблицы с данными, полученными из BIOS-Setup.

цы сегментов по разряду счетчика. Это объясняется тем, что счет может начинаться с 0 или с 1.

Кроме того, в качестве характеристики таблицы должно быть показание *0AA 55h*, на основании которого в процессе загрузки ПК распознается таблица сегментов.

Проще всего, если ранее на жестком диске был только единственный сегмент.

Обратите внимание на то, что для отдельных параметров может наблюдаться естественное расхождение между данными BIOS-Setup и табли-

- Если вы столкнулись с ошибкой, исправьте ее или связанное с ней значение и сохранитесь.

Если же ошибка связана с логическим диском, то с помощью программы PTS-Diskedit выделите в таблице сегментов поле *Type* строку *Extended* и нажмите клавишу [Enter]. Появится таблица логического диска, которая с технической точки зрения построена так же, как и таблица сегментов, и работает аналогично.

Если в результате проведенных мероприятий ПК «вернулся к жизни», то обязательно проведите контроль файловой системы (используя программу Scandisk), поскольку скорее всего ваши данные не будут полностью соответствовать оригиналу.

Обработал Сергей Зелинский/jk, fs, tw